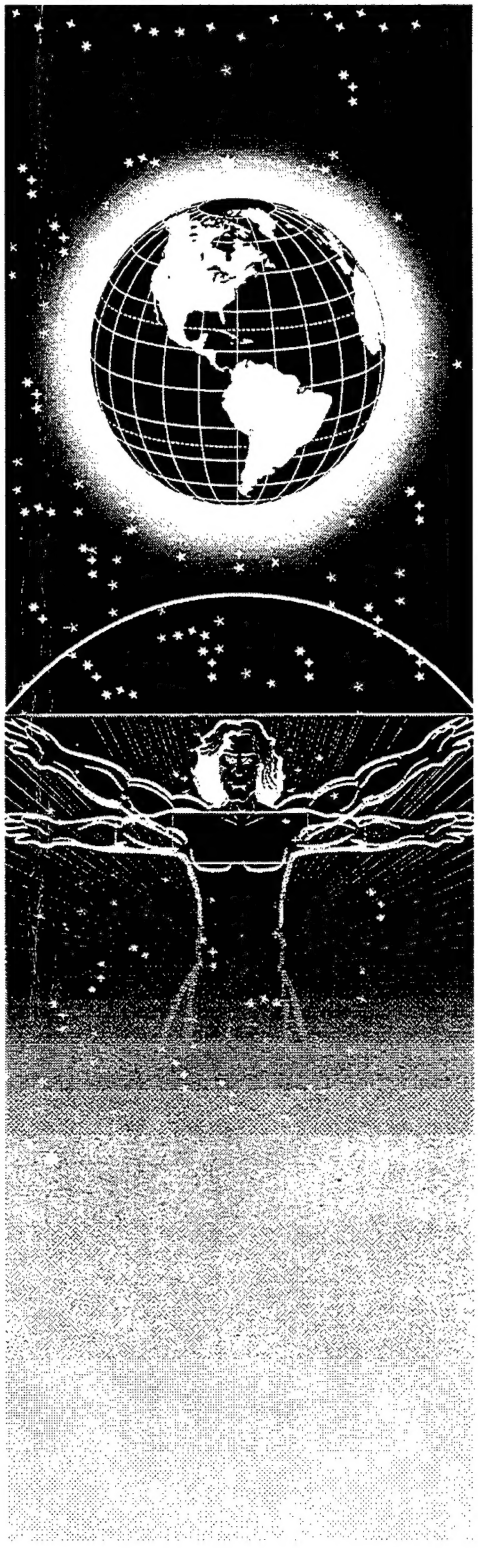
AFRL-HE-WP-TR-1998-0057



UNITED STATES AIR FORCE RESEARCH LABORATORY

EVENT SEQUENCE ANALYSIS OF THE AIR INTELLIGENCE AGENCY INFORMATION OPERATIONS CENTER FLIGHT OPERATIONS

Glen J. Larsen

ADROIT SYSTEMS, INC.
2970 PRESIDENTIAL DRIVE, SUITE 340
FAIRBORN OH 45324

APRIL 1998

INTERIM REPORT FOR THE PERIOD MARCH 1997 TO APRIL 1998

Human Effectiveness Directorate
Crew System Interface Division
Wright-Patterson AFB OH 45433-7022

NOTICES

When US Government drawings, specifications, or other data are used for any purpose other than a definitely related Government procurement operation, the Government thereby incurs no responsibility nor any obligation whatsoever, and the fact that the Government may have formulated, furnished, or in any way supplied the said drawings, specifications, or other data, is not to be regarded by implication or otherwise, as in any manner licensing the holder or any other person or corporation, or conveying any rights or permission to manufacture, use, or sell any patented invention that may in any way be related thereto.

Please do not request copies of this report from the Air Force Research Laboratory. Additional copies may be purchased from:

National Technical Information Service
5285 Port Royal Road
Springfield, Virginia 22161

Federal Government agencies registered with the Defense Technical Information Center should direct requests for copies of this report to:

Defense Technical Information Center
8725 John J. Kingman Road, Suite 0944
Ft. Belvoir, Virginia 22060-6218

TECHNICAL REVIEW AND APPROVAL

AFRL-HE-WP-TR-1998-0057

This report has been reviewed by the Office of Public Affairs (PA) and is releasable to the National Technical Information Service (NTIS). At NTIS, it will be available to the general public, including foreign nations.

This technical report has been reviewed and is approved for publication.

FOR THE COMMANDER

HENDRICK W. RUCK, PhD
Chief, Crew System Interface Division
Air Force Research Laboratory

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	April 1998	Interim, March 1997 to April 1998

4. TITLE AND SUBTITLE

Event Sequence Analysis of the Air Intelligence Agency Information Operations Center Flight Operations

5. FUNDING NUMBERS

C: F41624-94-D-6000
P: 62202F
PR: 7184
TA: 10
WU: 46

6. AUTHOR(S)

Glen J. Larsen

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Adroit Systems, Inc.
2970 Presidential Drive, Suite 340
Fairborn OH 45324

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Air Force Research Laboratory (AFRL)
Human Effectiveness Directorate
Crew System Interface Division
Air Force Materiel Command
Wright-Patterson AFB OH 45433-7022

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

AFRL-HE-WP-TR-1998-0057

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

This report applies Event Sequence Analysis, methodology adapted from aircraft mishap investigation, to an investigation of the performance of the Air Intelligence Agency's Information Operations Center (IOC) Flight Operations crew on duty at the time of the bombing of crew quarters in the Khobar Towers building in Dhahran, Saudi Arabia. The focus of the investigation is the identification of information gathering and information transfer activities that supported the formation of crew member decision making strategies. An assessment is made of the efficacy of these activities and their utility in supporting crew member situation awareness and the formulation of decisions under stress. The events under analysis are classified as tractable, relevant, and informational, in order to identify critical areas of interest. The report includes observations and recommendations for improving information flow (eliminating bottlenecks and duplications of effort), enhancing team performance and eliminating unnecessary stressors.

14. SUBJECT TERMS

Event Sequence Analysis, Critical Decision Method, Decision Making, Situation Awareness, Human Systems Integration, Information Warfare, Command and Control, C2, Information Operations, Information Protection, Terrorist Activities

15. NUMBER OF PAGES
28

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	Unlimited

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. Z39-18
298-102

This page intentionally left blank

PREFACE

The current paradigm for military operations, management, and decision making is captured in the definition of *command and control*:

> Command and Control (C2): the exercise of authority and direction by a properly designated commander over assigned or attached forces in the accomplishment of the mission; C2 functions are performed through an arrangement of personnel, equipment, communications, computers, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission.
>
> (JCS Joint Pub 1-02)

By contrast, the nature of the threat to national security and the key to dominant strategies and tactics of the future are embedded in the definition of *Information Age*:

> Information Age: the future time period when social, cultural, and economic patterns will reflect the decentralized, nonhierarchical flow of information; contrast this to the more centralized, hierarchical, social, cultural, and economic patterns that reflect the Industrial Age's mechanization of production systems.
>
> (Federation of American Scientists)

The challenge for success in the future is characterized by the observation that technology is progressing at a revolutionary pace while mankind only continues to evolve. Clearly, human performance cannot be an afterthought, particularly in the Information Operations Domain, which is dependent upon the analytical inputs of highly skilled individuals in critical areas (*e.g.*, the Defense Indications & Warning System). Thus, it is imperative that innovative training techniques and elegant decision making processes be employed to ensure that personnel perform optimally as individuals and as teams. The results are faster, more appropriate decisions with successful outcomes. Moreover, emphasis must be applied on doing things efficiently as well as effectively. Efficiency refers to doing things right, while effectiveness refers to doing the right things.

A model, postulated in 1992 to support optimal performance, is "Larsen's Law for Success" which states:

MAN + MACHINE + MISSION ≥ ENVIRONMENT

This project was completed for the Air Force Research Laboratory Information Analysis and Exploitation Branch (AFRL/HECA) under Air Force Contract F41624-94-D-6000, Work Unit 71841046—Crew Systems for Information Warfare, and directed by Logicon Technical Services, Inc., prime contractor. Mr. Donald Monk was Contract Monitor.

The author acknowledges and thanks Mr. Gilbert Kuperman (AFRL/HECA) for his initial interest and ongoing support for this project. The author also expresses his appreciation to the members of the Information Operations Center (IOC) at Air Intelligence Agency (AIA), Kelly AFB, Texas—especially Lt Col Dave Castillo, Mr. Lynn Reeves, 1Lt Dan Owen, MSgt Patrick Couture, and all those who participated in the information collection phase of this study.

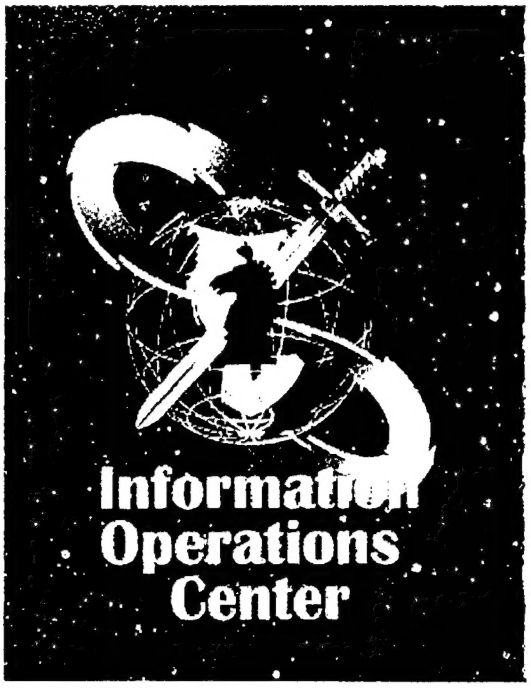

Information
Operations
Center

TABLE OF CONTENTS

Page

Introduction 1

Event Sequence Analysis Methodology 1

IOC Flight Operations Manning and Functions Assigned 3

Khobar Towers Event Sequence Activity 5

Observations and Recommendations 8

Appendix A: Sensor Mace 14

Glossary Of Terms 15

Definitions 17

References 21

LIST OF FIGURES

Page

Figure 1: Schematic of a Typical Accident Event Sequence List 3

Figure 2: Function Assignment Matrix 4

Figure 3: Scene at Khobar Towers after the Bombing 5

Figure 4: IOC Flight Operations Event Continuum (notional) 10

Figure 5: Process Integration for Information Superiority 12

LIST OF TABLES

Page

Table 1: Critical Decision Interview Probes 2

Table 2: Khobar Towers Event Sequence List, 25 June 1996 5

This page intentionally left blank

INTRODUCTION

The purpose of this report is to adapt Event Sequence Analysis, a method of analysis used in aircraft mishap investigation, in order to identify strategies and inferences necessary to support important and recurring decision making requirements within Information Operations. Ted W. Yellman, a Senior Principal Safety Analyst with Boeing Commercial Airplane Group, developed the methodology for Event Sequence Analysis. While the paradigm is generally used to analyze individual accidents, discover relevant causes, and identify changes to prevent future accidents, it will be adapted in this case to determine, if possible, what went right and what can be done to enhance performance.

The data for this analysis is provided generously by the Air Intelligence Agency (AIA) Information Operations Center (IOC) located at Kelly AFB, Texas. The IOC is the Air Force's multi-dimensional 24-hour operations center focusing on integrating and conducting worldwide information operations. Their capabilities include:

1. 24-Hour Help Desk for the Combat Intelligence System (CIS) and the USAF Intelink
2. Tactical Information Broadcast Service (TIBS)
3. Information Warfare (IW)/Command and Control Warfare (C2W) Planning Tools
4. Information Warfare Indications and Warning—CYBERWATCH
5. Operations Reachback through Requests for Information (RFI) and Exercise/Contingency Support
6. 24-Hour Point-of-Contact for AIA, an organization with over 16,000 personnel deployed worldwide

Specifically, this analysis will address the actions of the IOC Flight Operations crew on duty on 25 June 1996 during the shift that responded to the terrorist bombing that killed 19 service members at the Khobar Towers, near King Abdul Aziz Air Base, Dhahran, Saudi Arabia.

EVENT SEQUENCE ANALYSIS METHODOLOGY

Various methods exist for analyzing tasks performed in challenging environments. For example, the Critical Decision Method (CDM) is well suited for "modeling tasks in naturalistic environments characterized by high time pressure, high information content, and changing conditions" (Klein, Calderwood & MacGregor, 1989, p. 466). CDM is a technique that uses cognitive probes to elicit information from participants regarding situation assessment and decision making. Table 1 below describes various probes in detail (Klein et al., 1989).

Table 1 - Critical Decision Interview Probes

Probe Type	Probe Content
Cues	What were you seeing, hearing, smelling...?
Knowledge	What information did you use in making this decision, and how was it obtained?
Analogues	Were you reminded of any previous experience?
Goals	What were your specific goals at this time?
Options	What other courses of action were considered by or available to you?
Basis	How was this option selected/other options rejected? What rule was being followed?
Experience	What specific training or experience was necessary or helpful in making this decision?
Aiding	If the decision was not the best, what training, knowledge, or information could have helped?
Time Pressure	How much time pressure was involved in making this decision? (Scales vary)
Situation Assessment	Imagine that you were asked to describe the situation to a relief officer at this point—how would you summarize the situation?
Hypotheticals	If a key feature of the situation had been different, what difference would it have made in your decision?

As noted earlier, Ted W. Yellman applied his accident investigation paradigm to understand how a system will or will not work. Furthermore, the purpose of an accident investigation is to learn what went wrong, so we may attempt to prevent it from occurring in the future. An *Event Sequence List* is created to identify conditions and occurrences during the mission on which the accident occurred. The information for the list is compiled through the use of CDM techniques during interviews. The time continuum includes events that may or may not have occurred in either the pre-mission, mission, or post-mission phases. Events are classified as tractable, relevant, or informational. The definitions and their adaptations are as follows:

- **Tractable Events**: an event that can be eliminated or reduced in frequency in the future resulting in improved performance.
- **Relevant Events**: relate to events that are possible causes of the accident and *tractable.* Adapted version—events that may or may not support the successful completion of a particular task or mission-related objective
- **Informational Events**: events that are not relevant, but important to understanding the phenomena during the accident sequence.

Figure 1 below graphically depicts a typical Event Sequence List. Note that the example does not show the post-mission phase, since it is precluded by an accident (i.e., "Tragic Result;" Yellman, 1997).

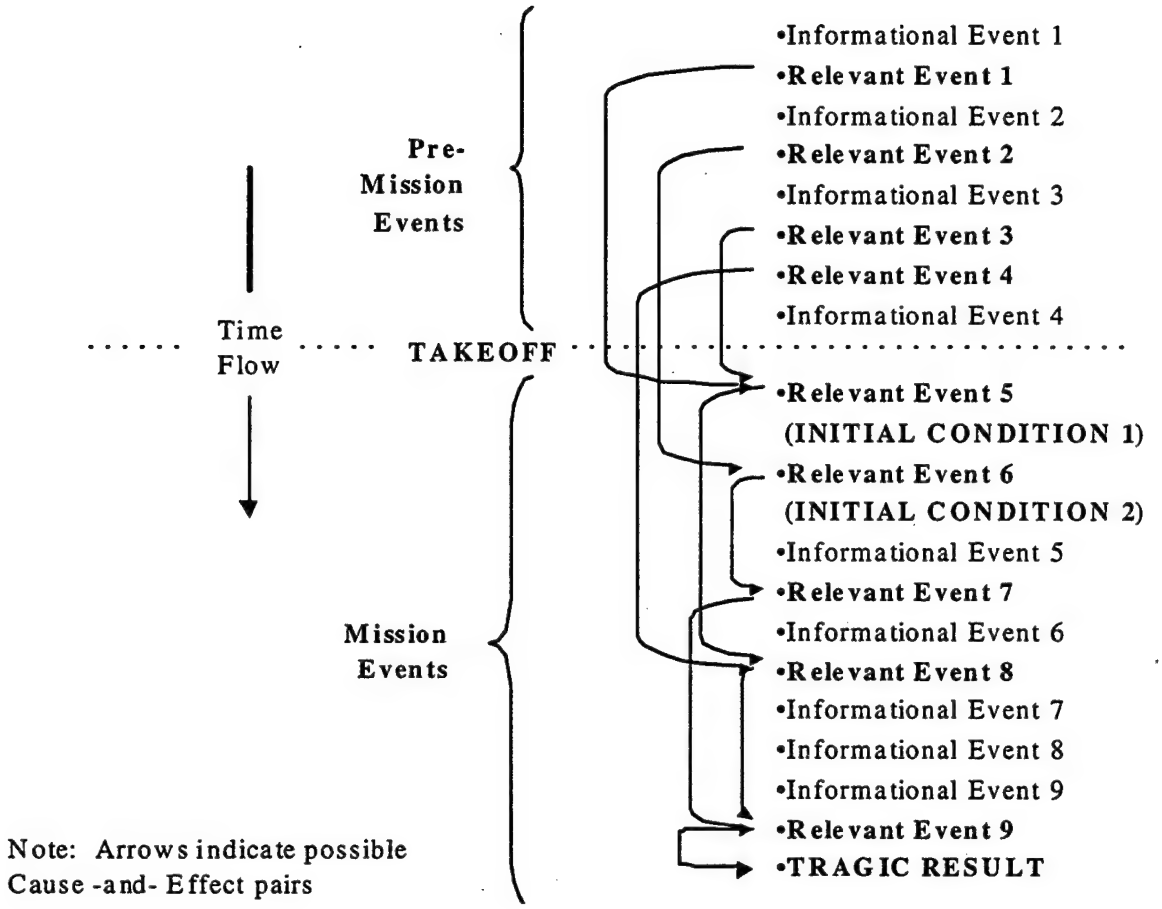


Figure 1: Schematic of a Typical Accident Event Sequence List

For the purpose of this report, the time continuum will begin at 0600, which is the start of the shift. However, pre-mission events could include activities such as driving to work, eating breakfast, any sleep disturbances, or various stressors that may have an impact on the crew(s) performance during the mission. Initial conditions identified in the following event sequence list relate to starting points for particular tasks to be performed or mission-related objectives. Results indicate the outcome of a series of events. In addition, mission events can include those activities which occur after a mission is accomplished, such as debriefings and critique sessions.

IOC FLIGHT OPERATIONS MANNING AND FUNCTIONS ASSIGNED

On the date of the incident, the IOC Flight Operations crew included eight US Air Force personnel: one Watch Officer, one Mission Supervisor, three Flight Analysts, two Tactical Electronic Order of Battle (TEOB) Analysts, and one Combat Intelligence System technician.

The Watch Officer is typically a junior intelligence officer (lieutenant) who serves as the crew's senior analyst responsible for setting the flight objectives and integrating all flight activities. The Mission Supervisor is typically a senior non-commissioned intelligence officer

(master sergeant or above) responsible for managing the flight personnel and supervising tasks performed. Flight Analysts are generally junior airmen who have recently completed intelligence technical training at Goodfellow AFB, Texas. The TEOB Analysts are more experienced airmen or junior non-commissioned officers responsible for analyzing electronic intelligence and employing the SENSOR MACE system (see Appendix A). The CIS Technician is usually a junior non-commissioned officer responsible for manning the CIS Help Desk to support USAF personnel worldwide who use CIS. Figure 2 below depicts a matrix of duties performed during the crew's twelve-hour work schedule on 25 June 1996.

Information Operations Center
Flight Operations
Assignment of Functions

Function Assigned \ Operator Assigned	Watch Officer	Mission Supervisor	Flight Analysts	TEOB Analysts	CIS Help Technician
Situation Manager	X				
Personnel Manager		X			
Research			X	X	
Briefing Prep	X		X	X	
Communications/ ZIRCON Chat			X		
AIA Internal Coordination	X				
Coordination with outside agencies		X			
Receive RFIs			X		
Assign/Prioritize RFIs		X			
Message(s) receipt			X		
Quick Reaction Checklists (QRC)	X	X			
Incoming Phone Calls			X	X	
Fax RX/TX			X		
CIS Help Desk					X

Figure 2: Function Assignment Matrix

The scene at Khobar Towers after the bombing is shown in Figure 3. The re-creation of the Flight Operations activities and significant events surrounding the Khobar Towers bombing are listed in Table 2.

KHOBAR TOWERS EVENT SEQUENCE ACTIVITY

Figure 3: Scene at Khobar Towers after the Bombing

Table 2: Khobar Towers Event Sequence List, 25 June 1996

Time	Activity	Event Type
Pre-0600	Pre-mission Phase: On-coming crew traveled to the IOC to start work. All reported on time, with no significant occurrences.	Informational
0600	"Pass On" (crew change)—Begin Mission	Initial Condition
	Crew change included: A Watch Officer, a Mission Supervisor, 3 Flight Analysts, 2 TEOB Analysts, and a CIS Help Technician	Relevant
	Routine discussion—no briefing requirement for the day Reviewed email, administrative tasks, daily announcements	Informational
	Read current intelligence traffic	Informational
	Received routine phone calls (people looking for others, asking for connections or non-specific current intelligence questions)	Tractable
	The crew was very interested in the current Bosnian theater activities	Relevant
	Monitored the Joint Worldwide Intelligence Communication System	Informational

Time	Activity	Event Type
	(JWICS) and Requests for Information (RFIs)	
	CNN Headline News (monitored continuously)	Relevant
	Sensor Mace – continuously monitored	Informational
1100	Lunch—staggered to ensure personnel are available for required tasks (no lunch hour per se, people get their food and eat it "on flight")	Informational
1500	Received message re: bombing at Khobar Towers—casualties unknown, damage unknown	Initial Condition
	Flight Analyst called the National Military Joint Intelligence Center (NMJIC) to confirm the event and were told to go away, they're too busy	Relevant
	One flight analyst assigned to check the Reuters terminal	Relevant
	One flight analyst assigned to query the X-Windows (Version) Threat Analysis Reporting System (XTARS) for any message traffic re: Khobar Towers	Relevant
	One flight analyst assigned to do Intelink search for relevant information and message traffic	Relevant
1510	Watch Officer and the analyst using Reuters established a ZIRCON chat (see Glossary) with the CSG (Communications Security Group) at Riyadh, Saudi Arabia to relay Khobar Towers information.	Relevant
	IOC called Dhahran but the DSN system (used for DoD long distance phone calls) was down	Relevant
	Based on ZIRCON chat w/CSG, AIA/IOC offered pertinent information to NMJIC & US Central Command (CENTCOM)	Result
	Watch Officer began telephone notifications in AIA chain of command as well as local command posts (Kelly AFB, Lackland AFB) in accordance with Quick Reaction Checklist (QRC)	Informational
1530	IOC received AIA/DO (Director of Operations) tasking: • call AIA/DP (Director of Personnel) for list of AIA people in the area • make space for 2 to 3 people from the 67th Intelligence Wing (IW), supporting IOC • coordinate with AF Casualty Center at Randolph AFB to relay appropriate information • prepare briefing on current situation for presentation at 1800	Relevant Initial Condition
1545	Air Force Information Warfare Center Commander (AFIWC/CC) entered IOC and asked for update. The Watch Officer gave him a quick SITREP and the AFIWC/CC departed.	Tractable
	AIA Public Affairs (PA) called the IOC and provided a central hotline number for family members to call for news regarding the bombing incident; another hotline number was provided for press queries.	Relevant
1600	NOTE: unknown to the IOC crew, at about this time the AIA/DO	

Time	Activity	Event Type
	called the organization's senior staff, informing them of the current situation and that the IOC would provide a briefing at 1800; until then people were to let the IOC do their job and not interfere.	Relevant
	3 individuals from the 67th IW (a Captain, a Master Sergeant (MSgt), and a Technical Sergeant (TSgt) arrived to help IOC taskings	Relevant
	A Flight Analyst was assigned by the Mission Supervisor to help the Captain and MSgt make required telephone calls in accordance with (IAW) the QRC	Relevant
	The 67th IW TSgt was released and sent home to rest in order to return for the night shift at 2200 hours	Tractable
	The Watch Officer and Mission Supervisor decided to call the on-coming Watch Officer and Mission Supervisor at their home and request that they come in at 1700 (an hour earlier than scheduled) in order to facilitate "Pass On"	Relevant
	The IOC called AIA associated units to inquire if they had any personnel in the Khobar Towers area	Relevant
	Work continued on compiling the AIA personnel list, including total number of personnel, unit assigned, and their location in Dhahran	Informational
1630	IOC started developing the 1800 crisis briefing for the AIA/DO and senior staff	Informational
	Individuals were assigned tasks to get imagery of the bombing site and review available intelligence sources	Relevant
	One TEOB Analyst was directed to focus attention on Electronic Intelligence (ELINT) of geographic areas where bombing suspects might be located	Relevant
	The other TEOB Analyst continued normal duties	Informational
	The CIS Help Technician used CIS as another communications tool to gain additional information on the Dhahran situation	Relevant
	The IOC received numerous telephone queries during this period	Tractable
	The 67th IW augmentees primarily answered the phones and coordinated the current status with subordinate AIA commanders	Relevant
1700	CNN announced the Khobar Towers bombing and showed the first pictures of the event	Initial Condition
	The on-coming Watch Officer and Mission Supervisor arrived	Informational
	The IOC called the Air Force Casualty Center to correct the CNN report regarding the number of casualties	Relevant
	The IOC informed the AIA/DO and IOC Director of the CNN coverage.	Informational
	A local TV News station called and was directed to the press hotline.	Tractable
	The on-coming Watch Officer and Mission Supervisor generally observed the activities and helped field some phone calls.	Informational
1755	The 1800 briefing was finalized for presentation.	Informational
1800	The AIA/DO Briefing was presented in the IOC Conference Room;	

Time	Activity	Event Type
	attendees included the AIA/DO, the AFIWC/CC, the Director of PA, and senior staffers.	Relevant
	The briefing included: 1. Khobar Towers situation update 2. Current casualty numbers 3. Accountability list of AIA people in the Dhahran area 4. Ongoing IOC activities 5. Intelligence update regarding activities of suspect nations/groups	Result
	The IOC crew change occurred, except for the Watch Officer and Mission Supervisor	Relevant
1815	AIA/DO set the next briefing time for 0600 on the following morning	Informational
1820	AIA/PA stated they would not be manned 24 hours, but provided a point of contact, if necessary.	Informational
1830	The Watch Officer and Mission Supervisor began official "Pass On" to the next crew and stressed the importance of getting Khobar Towers imagery for the 0600 briefing.	Relevant
	The Watch Officers and Mission Supervisors reviewed the "Pass On" log together to ensure completeness and address any areas of concern.	Relevant
1900	The day shift Watch Officer and Mission Supervisor departed the IOC, after deciding to arrive at 0500 (1 hour early) for the next day's shift.	Relevant
	NOTE: the AIA Dhahran personnel accountability list was not finalized until approximately 2200	Informational

OBSERVATIONS AND RECOMMENDATIONS

Observation 1: By chance, the crew on duty during this terrorist bombing was the most experienced crew at the IOC. Consequently, decisions that might have required more discussion and research by inexperienced crews were made decisively and quickly. The event sequence list might have been dramatically different but for the crew on duty.

Recommendation 1: Ensure training programs incorporate this event as a lesson of benchmarked performance. Moreover, continuation-training sessions should include exercises on response to crisis situations.

Observation 2: Only the Watch Officers and Mission Supervisors reviewed the "Pass On" log at shift changeover.

Recommendation 2: The entire on-coming crew should participate in the review and discussion of the "Pass On" log in order to build greater situational awareness and team cohesiveness.

Observation 3: Availability of the ZIRCON chat system and decision to use it were critical success factors in the crew's efforts.

Recommendation 3: Ensure IOC flight operations crews regularly use ZIRCON to communicate with other units as a means of exercising the system for crew proficiency, to communicate center status, and to share the intent of theater commanders in order to properly focus attention on priority issues. This action will serve to strengthen relationships among various operations centers, resulting in greater synergy and effectiveness.

Observation 4: The AIA Director of Operations acted in a manner that significantly facilitated the smooth performance of the IOC flight operations crew. However, sending the additional personnel from the 67th IW to augment the crew was unexpected and unplanned.

Recommendation 4: To the extent practical, ensure the IOC concept of operations (CONOPS) is coordinated and reviewed by the AIA/DO, as well as lateral and supporting organizations to preclude hidden expectations and maximize contingency planning.

Observation 5: From an ergonomic perspective, the IOC flight operations work area does not appear to promote efficient performance of assigned tasks. For example, analysts must use several different computer systems in separate locations around the work area to access desired information. Moreover, numerous monitors that continuously display information cannot be seen easily, or at all, depending on where the individual is working (Human Systems Integration Seminar, 1996).

Recommendation 5: Given the unit's mission, the IOC should conduct a Human Systems Integration Analysis to consider the critical elements that determine the optimum design and lowest impact on total life cycle costs of the IOC system. For the safety, effectiveness, affordability, capability, survivability, and operability of the system to be optimum, the effect of the hardware on the human, as well as the effect of the human on the hardware, must be considered key to the final design of the total system. The idea is to equip the man, not man the equipment. To do otherwise will force "work-arounds," inefficiency, and excessive costs (Booher, 1990).

Undoubtedly, the warriors of the 21st Century will be the most informed war-fighters of all time. These modern warriors will have the latest available intelligence data, enhanced communications, manned and unmanned support equipment and will control troops from a greater distance over a wider variety of missions. Requirements, resources, systems, and applications are still being developed, particularly from the perspective of Human Systems Integration (HSI). The majority of these systems are focused on obtaining an accurate prediction of pending actions, or modifying how the military leaders, civilians, decision makers, and the warfighters react, or aiding the commander in the decision making process. Effective information warfare systems need to replicate and predict human cognitive processes to include cross-cultural modeling. Increased employment of information warfare systems will heighten the requirement for robust, engineered tools that are based on advanced human systems integration requirements. HSI is defined as a comprehensive management and technical approach for addressing the human-centered elements of manpower, personnel, training, safety, health

hazards, survivability, and human factors engineering in the acquisition of new or improved systems. Thus, system performance is a function of human performance, equipment performance, and the environment.

$$P_S = f[(P_h)(P_e)(E)]$$

Observation 6: On the basis of interviews for this report, it appears that flight operations crews tend to work together as a group, as opposed to working as a team. Typically, a group is composed of individuals who perform their specific tasks apart from other members of the group and who contribute their work to the group's total product. By contrast, a team is composed of individuals who must work in unison to achieve the objectives of the team. Although experienced individuals who work together over long periods of time may develop the kinds of behavior that fosters teamwork, such an outcome will generally not occur unless a teambuilding system is in place (Katzenbach & Smith, 1993).

Recommendation 6: Adapt Air Force Instruction (AFI) 36-2243, *Cockpit/Crew Resource Management (CRM) Program, June 1994* (currently in re-write as AFI 11-290) for use in Information Operations. CRM is defined as "the effective use of all available resources—people, weapon systems, facilities, equipment, and environment—by individuals or crew to safely and efficiently accomplish an assigned mission or task" (*AFI 36-2243*, 1994, p.7). While the AFI mandates CRM training for USAF aircrews, it points out that the underlying principles of CRM can be applied to any functional area requiring the performance of time critical tasks by individuals within the framework of a team. Numerous studies have validated the role CRM plays in improving crew performance and increasing mission effectiveness. IOC Flight Operations crews could employ the core concepts of CRM during their missions as depicted in Figure 4 (*AFI 36-2243*, 1994).

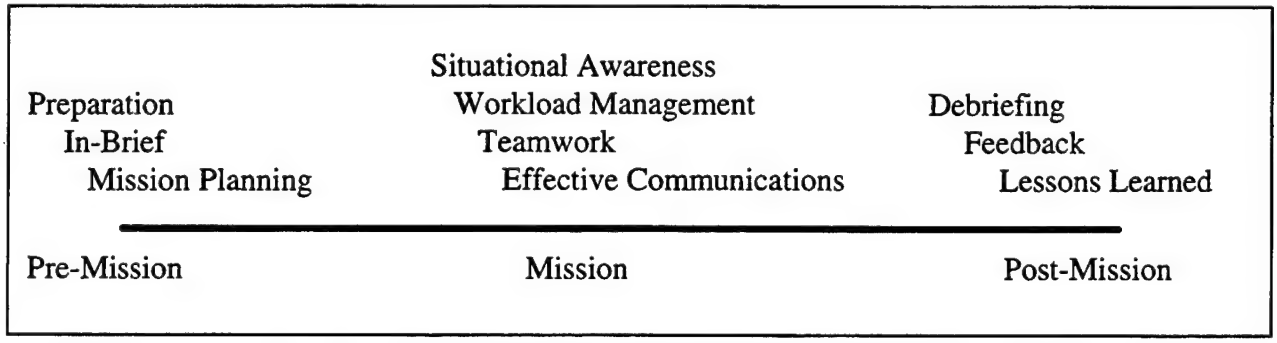


Figure 4 - IOC Flight Operations Event Continuum (notional)

Observation 7: Given the nature of the emerging Information Warfare threat, IOC Flight Operations must remain vigilant for indications of communications penetrations as exemplified in ELIGIBLE RECEIVER 97, the first major DoD exercise focused on Information Warfare. An observation noted by the Joint Staff indicated that when trouble tickets were called into the J2 Help desk personnel and supervisors were not aware of the ongoing exercise and possible IW

threats to NORAD-USSPACECOM (N-SP) intelligence systems and communications systems. When numerous trouble tickets were called into the Help Desk, they could have been indications of an ongoing IW/cyber attack against our command and control, communications, computers and information (C4I) infrastructure. A recommendation was made to develop a Defensive IW CONOPS and to train personnel on methods to identify when systems and communications networks may be under attack or penetration, and secondly, to identify what immediate action responses are required to minimize or stop damages from occurring. Additionally, information about pending or ongoing exercises should be more widely disseminated throughout the Joint Staff Intelligence Directorate (J2). Although there may not be direct involvement by a specific J2 branch or division, it does not preclude the responsibility to have situational awareness on what other members of the J2 are doing. From the perspective of the Air Intelligence Agency IOC, this directly applies to the CIS Help Desk, which provides 24-hour-a-day support to field units deployed throughout the world (JWFC, 1997).

Recommendation 7: In order to maintain situational awareness, it would be appropriate to note ongoing major Joint and Air Force exercises in the "Pass On" log to include their participants.

Observation 8: A significant conclusion of ELIGIBLE RECEIVER 97 was that USSPACECOM is going to play a key leadership role in the conduct of DoD Information Operations (IO). Moreover, if the J2 Staff is to be fully supportive of this evolution of the modern battlefield, and the USSPACECOM Commander's desires, then the Combat Intelligence Center (CIC) must provide IO support to the same extent as is provided for space systems and missiles. It was recommended that the CIC should gather, document, and maintain foreign IO reliance and capabilities, using the standing Country Files J2 is currently developing and maintaining.

Recommendation 8: While the IOC coordinates its activities with the CIC as necessary, it appears that a regular, daily process of sharing information regarding the IW indicators identified in the Defense Indications and Warning System (DIWS) could enhance the capability to predict and effectively warn of IW attacks on the Defense Information Infrastructure (DII; Commission on Critical Infrastructure Protection, 1997).

Observation 9: Compartmentalization of intelligence information has been a fact of life due to security classification issues. Information Warfare has dramatically challenged the intelligence community to respond at the speed of electronic media. The integration of information to enable effective decision making is a critical element of successful military operations. While technology is marching forward with more robust information systems, the decisions to act and to engage still reside between the ears of people, whether they are commanders, aircrew members, or information operators (Office of the Under Secretary of Defense for Acquisition & Technology, 1996).

Recommendation 9: Develop integrative models of well-known decision and production processes, such as those identified in Figure 5 to ensure information operators achieve desired objectives. If the techniques of "imagineering" ensured the success of Disney World, it's sure worth a try in the "Cyber World." Imagineering is a term coined by the Disney Corporation to denote the combination of imagination and engineering to create the enormously successful attractions in its theme parks. It represents the kind of "outside the box" thinking that is

necessary to maintain our competitive edge in the ongoing Revolution in Military Affairs (Lefkon, 1996; *AFDD 1*, 1997).

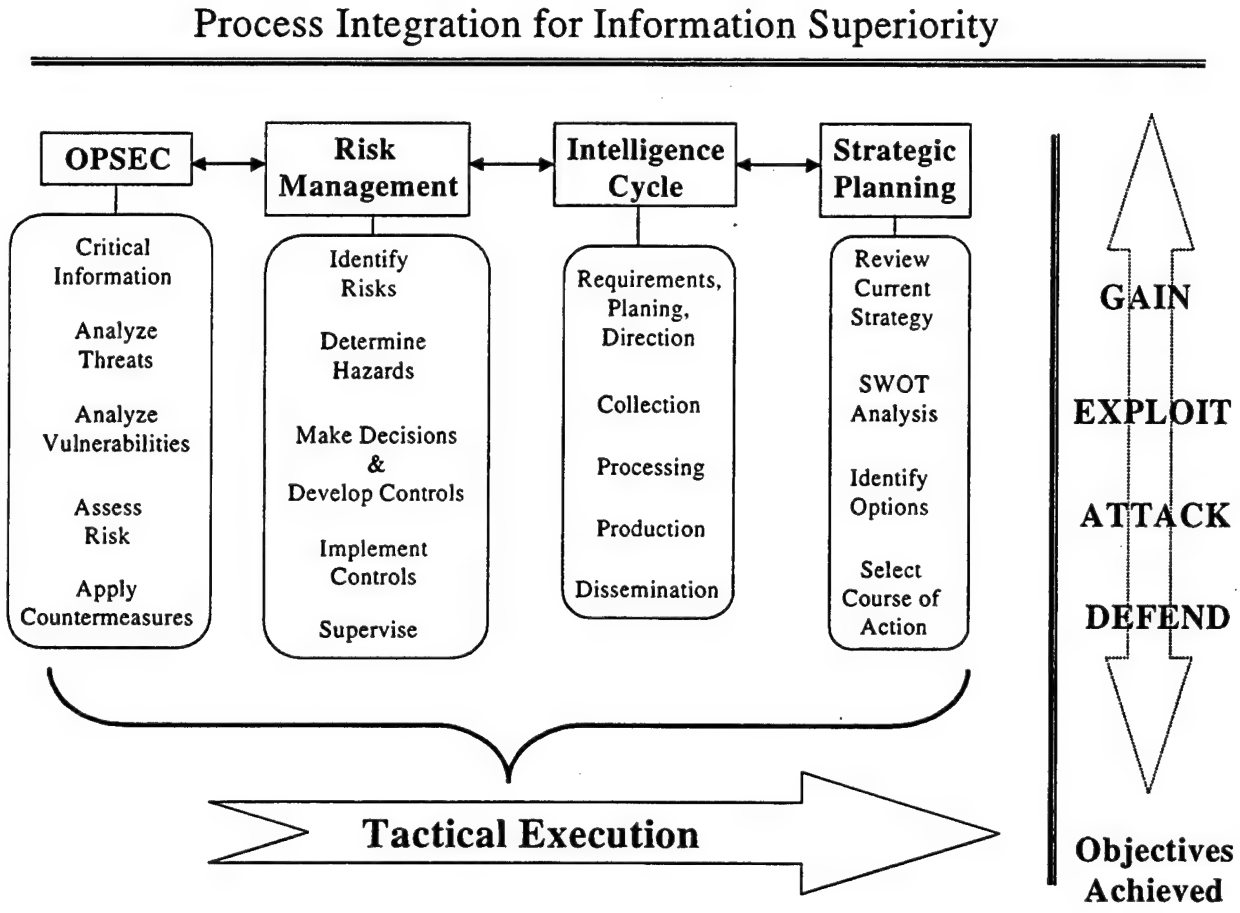


Figure 5 – Process Integration for Information Superiority

According to *Air Force Doctrine Document 1*, Information Superiority "is the ability to collect, control, exploit, and defend information while denying an adversary the ability to do the same and, like air and space superiority, includes gaining control over the information realm and fully exploiting military information functions" (1997, p. 31). Information Superiority is an Air Force core competency directly supported by the Air Intelligence Agency (AIA). As stated in the *Air Intelligence Agency 1997 Almanac*, the AIA vision is "The Air Force leader in integrating and conducting information operations that shape the international security environment and, when necessary, the battlespace. Securing and maintaining information dominance for the decision maker...from the individual warfighter to the commander in chief" (*AIA Almanac*, p. 67). AIA considers information operations as a continuum of options that include gaining, exploiting, attacking, or defending information. The decision to pursue any one of those options depends on mission objectives and the commander's intent (AIA Almanac, 1997, p. 3).

In order to achieve Information Superiority, Figure 5 presents four key processes that must work in unison so that: 1) appropriate courses of action can be identified, 2) a particular

course may be chosen by the commander, and 3) tactics be developed that enable the achievement of stated objectives.

In particular, Operations Security (OPSEC) is a key process because it allows the identification of critical information regarding military operations that must be protected (Interagency OPSEC Support Staff, 1996). Risk Management classically is concerned with the process of making operations safer without compromising the mission. The bottom line is that risks should not be taken if the benefits do not outweigh the costs. In addition, the intelligence cycle must operate both simultaneously and in conjunction with the use of OPSEC and Risk Management, so that information is used efficiently. Moreover, any information gaps identified in the process would naturally trigger further intelligence requirements. Each of these processes is a critical contributor to any strategic plan, regardless of scale. However, a strategic plan is just a plan unless effective tactics are chosen to execute it.

APPENDIX A: SENSOR MACE

SENSOR MACE was developed by BTG, Inc. (a defense contractor, headquartered in Fairfax, VA) as a prototype for the Air Force Information Warfare Center to demonstrate Information Warfare capabilities and is now the mainstay for the Center's operations. SENSOR MACE provides real time message handling, correlation of multiple disciplines of intelligence data, and automatic database updating. SENSOR MACE is capable of secondary imagery analysis through the use of electronic light table (ELT) or Demand-Driven Direct Digital Dissemination System (5-D) imagery applications.

The SENSOR MACE program grew out of the Constant Source maintenance program in order to provide the AFIWC with rapid prototyping for systems and software development. Key to the success and continuation of the program is a strict adherence to open system standards, allowing BTG to provide accurate and reliable systems development that are of a "plug and play" nature. This is critical to AFIWC because of the need to access various networks and databases at different stages of security to provide nodal analysis for Constant Web. SENSOR MACE provides C2 support by allowing commanders and analysts to access multiple intelligence databases. (Information is available on line at: **ww.btg.com/btg_home/customer/s_storys.htm**)

GLOSSARY OF TERMS

5-D	Demand-Driven Direct Digital Dissemination System
AFI	Air Force Instruction
AFIWC	Air Force Information Warfare Center
AFIWC/CC	Air Force Information Warfare Center Commander
AIA	Air Intelligence Agency
C2	Command and Control
C2W	Command and Control Warfare
C4I	Command, Control, Communications, Computers, and Intelligence
CDM	Critical Decision Method
CENTCOM	Central Command
CIC	Combat Intelligence Center
CIS	Combat Intelligence System
COE	Common Operating Environment
CONOPS	Concept of Operations
CSG	Communication Security Group
DII	Defense Information Infrastructure
DISN	Defense Information System Network
DIWS	Defense Indications and Warning System
DO	Director of Operations
DP	Director of Personnel
ELINT	Electronic Intelligence
ELT	electronic light table
HSI	Human Systems Integration
IAW	in accordance with
IO	Information Operations
IOC	Information Operations Center
IW	Information Warfare or Intelligence Wing
J2	Joint Staff Intelligence Directorate
JWICS	Joint Worldwide Intelligence Communications System

NMJIC	National Military Joint Intelligence Center
NORAD	North American Air Defense Command
N-SP	NORAD-USSPACECOM
OPSEC	Operations Security
PA	Public Affairs
QRC	Quick Reaction Checklist
RFI	Request for Information
SITREP	Situation Report
SWOT	Strengths, Weaknesses, Opportunities, and Threats
TEOB	Tactical Electronic Order of Battle
TIBS	Tactical Information Broadcast System
USSPACECOM	United States Space Command
XTARS	X-Windows (Version) Threat Analysis Reporting System
ZIRCON	A classified internet relay chat (IRC) program connected to the Joint Worldwide Intelligence Communications System (JWICS)

DEFINITIONS

Pertinent definitions are taken from the glossary of Army Field Manual 100-6: Information Operations. An electronic copy can be found through the Federation of American Scientists (FAS) web page at **http://www.fas.org/irp/doddir/army/fm100-6/glossary.htm**, unless noted otherwise:

Command and control: the exercise of authority and direction by a properly designated commander over assigned or attached forces in the accomplishment of the mission; C2 functions are performed through an arrangement of personnel, equipment, communications, computers, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission (*JCS Joint Pub 1-02,* 1998)

Command and control-attack: the synchronized execution of actions taken to accomplish established objectives that prevent effective C2 of adversarial forces by denying information to, by influencing, by degrading, or by destroying the adversary C2 system

Command and control-protect: the maintenance of effective C2 of own forces by turning to friendly advantage or negating adversary efforts to deny information to, to influence, to degrade, or to destroy the friendly C2 system; C2-protect can be offensive or defensive in nature; offensive C2-protect uses the five elements of C2W to reduce the adversary's ability to conduct C2-attack; defensive C2-protect reduces friendly C2 vulnerabilities to adversary C2-attack by employment of adequate physical, electronic, and intelligence protection (*US Army FM 100-6*, 1996)

Command and control system: the combination of personnel, equipment, communications, computers, facilities, and procedures employed by the commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission; the basic functions of a command and control system are sensing valid information about events and the environment, reporting information, assessing the situation and associated alternatives for action, deciding on an appropriate course of action, and ordering actions in correspondence with the decision (*JCS Joint Pub 1-02*, 1998)

Command and control warfare: the integrated use of operations security, military deception, psychological operations, electronic warfare, and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary C2 capabilities, while protecting friendly C2 capabilities against such actions; command and control warfare applies across the operational continuum and all levels of conflict (*JCS Joint Pub 1-02*, 1998)

Common operating environment: an environment that provides a familiar look, touch, sound, and feel to the commander, no matter where the commander is deployed; information presentation and command, control, communication, computers, and intelligence system interfaces are maintained consistently from platform to platform, enabling the commander to focus attention on the crisis at hand; also called COE

Communications security: the protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the possession and study of telecommunications or to mislead unauthorized persons in their interpretation of the results of such possession and study; also called COMSEC; includes cryptosecurity, transmission security, emission security, and physical security of communications security materials and information

Computer security: involves the measures and controls that ensure confidentiality, integrity, and availability of the information processed and stored by a computer; these include policies, procedures, and the hardware and software tools necessary to protect the computer systems and the information processed, stored, and transmitted by the systems

Counterintelligence: those activities which are concerned with identifying and counteracting the threat to security posed by hostile services, organizations, or by individuals engaged in espionage, sabotage, subversion, or terrorism (*JCS Joint Pub 1-02*, 1998)

Critical information: specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment (*JCS Joint Pub 1-02*, 1998)

Defense information infrastructure: the shared or interconnected system of computers, communications, data, applications, security, people, training, and other support structures serving DoD's location and worldwide information needs; the DII connects DoD mission support, command and control, and intelligence computers and users through voice, data, imagery, video, and multimedia services and provides information processing and value-added services to subscribers of the Defense Information System Network (DISN)

Information: data collected from the environment and processed into a usable form

Information Age: the future time period when social, cultural, and economic patterns will reflect the decentralized, nonhierarchical flow of information; contrast this to the more centralized, hierarchical, social, cultural, and economic patterns that reflect the Industrial Age's mechanization of production systems

Information data bases: an information visualization system that allows commanders and units to continually access and update a common database of relevant information (for example, logistics, intelligence, movement)

Information dominance: the degree of information superiority that allows the possessor to use information systems and capabilities to achieve an operational advantage in a conflict or to control the situation in operations other than war while denying those capabilities to the adversary

Information operations: continuous military operations within the military information environment that enable, enhance, and protect the friendly force's ability to collect, process, and act on information to achieve an advantage across the full range of military operations; information operations include interacting with the global information environment and exploiting or denying an adversary's information and decision capabilities

Information security: the protection of unauthorized access to or modification of information, whether in storage, processing, or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats

Information systems: the entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information (*JCS Joint Pub 6-0*, 1995)

Information systems security: a composite means to protect telecommunications systems and automated information systems and the information they transmit and/or process

Information warfare: actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems and computer-based networks (*Joint Pub 1-02*, 1998)

INFOSEC: information security

Infosphere: the rapidly growing global network of military and commercial command, control, communications, and computer systems and networks linking information data bases and fusion centers that are accessible to the warrior anywhere, anytime, in the performance of any mission; provides the worldwide automated exchange-of-information backbone support to joint forces; and provides seamless operation from anywhere to anywhere that is secure and transparent to the warrior; this emerging capability is highly flexible to support the adaptive command and control infrastructures of the twenty-first century

Intelligence: the product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas; also, information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding (*JCS Joint Pub 1-02*, 1998)

Military information environment: the environment contained within the global information environment, consisting of information systems and organizations, both friendly and adversary, military and nonmilitary, that support, enable, or significantly influence a specific military operation

Operations security: a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities; identifying those actions that can be observed by adversary intelligence systems; determining indicators adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and selecting and executing measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation; also called OPSEC

Relevant common picture of the battlefield: the aggregate of data that is shared among all friendly forces on the disposition of friendly and enemy force; this data is used to build a tailored

Relevant graphic display for the warfighter that increases in detail shown as the echelon served is closer to the soldier; commonly called situational awareness

Relevant information: information drawn from the military information environment that significantly impacts, contributes to, or is related to the execution of the operational mission at hand

Strategic plan: a comprehensive statement of an organization's strategic mission, objectives, and strategy; a detailed road map of the direction and course the organization presently intends to follow in conducting its activities (Thompson & Strickland, 1987).

REFERENCES

Air Force Doctrine Document 1 (AFDD 1): Air Force Basic Doctrine, September 1997. Washington, DC: US Air Force, AFDC/DR. Available: **http://www.dtic.mil/doctrine/jel/service_pubs.htm**

Air Force Instruction 36-2243 (AFI 36-2243): Cockpit/Crew Resource Management (CRM) Program, June 1994 (in revision as AFI 11-290). Washington, DC: US Air Force, XOOT.

Air Intelligence Agency (1997). AIA in review, '97. *AIA Almanac, 4*(1), 67.

Air Intelligence Agency (1997). Foreward, '97. *AIA Almanac, 4*(1), 3.

Booher, H. R., Ed. (1990). *MANPRINT: An Approach To Systems Integration.* New York, NY: Van Nostrand Reinhold.

Commission on Critical Infrastructure Protection (1997). *Critical Foundations: Protecting America's Infrastructures: The Report of the President's Commission on Critical Infrastructure Protection, 13 October 1997.* Washington, DC: Government Printing Office.

Defense Science Board (1996). *Report of the Defense Science Board Task Force on Information Warfare–Defense (IW-D), November 1996.* Washington, DC: Department of Defense, Office of the Under Secretary of Defense for Acquisition & Technology.

ELIGIBLE RECEIVER 97. Ft. Monroe, VA: Joint Warfighting Center (JWFC), Joint Center for Lessons Learned. Available: **http://www.jwfc.js.mil/pages/jel1.htm** (.mil sites only).

Briefing slides and personal notes. *Human Systems Integration Seminar*, United States Air Force Human Systems Center, Brooks Air Force Base, 8 June 1996. For further information on HSI, contact HQ HSC/XRC, 2510 Kennedy Circle, Suite 220, Brooks AFB, TX 78235, (210) 536-6401.

Interagency OPSEC Support Staff (1996). *Intelligence Threat Handbook, Revised May 6, 1996.* Greenbelt, MD: Author. To request a copy, call (800) 688-6115.

Joint Chiefs of Staff Joint Publication 1-02 (JCS Joint Pub 1-02): DoD Dictionary of Military and Associated Terms, as Amended 28 Jan. 1998. Available: **http://www.dtic.mil/doctrine/jel/c_pubs.htm**

Joint Chiefs of Staff Joint Publication 6-0 (JCS Joint Pub 6-0): Doctrine for C4 Systems Support to Joint Operations, May 30, 1995. Available: **http://www.dtic.mil/doctrine/jel/c_pubs3.htm.**

Katzenbach, J. R. & Smith, D. K. (1993). The discipline of teams. *Harvard Business Review, 71*(2), 111-120.

Klein, G. A., Calderwood, R., & MacGregor, D. (1989). Critical decision method for eliciting knowledge. *IEEE Transactions on Systems, Man, and Cybernetics, 19*(3), 462-472.

Lefkon, Wendy, Ed. (1996). *Walt Disney Imagineering: A Behind the Dreams Look at Making the Magic Real.* New York: Hyperion.

Thompson, A. A. & Strickland, A. J. III (1987). *Strategic Management: Concepts and Cases.* Plano, TX: Business Publications, Inc.

US Army Field Manual 100-6 (FM 100-6): Information Operations, 27 August 1996. Washington, DC: US Army.

Yellman, T. W. (July-September 1997). Learning from an accident. *ISASI Forum*, 25-30.